

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-010044

(43)Date of publication of application : 11.01.2002

(51)Int.Cl.

H04N 1/21
G06F 3/06
G06F 3/08
G06K 19/10
G06K 19/07
// H04L 9/32

(21)Application number : 2000-184993

(71)Applicant : CANON INC

(22)Date of filing : 20.06.2000

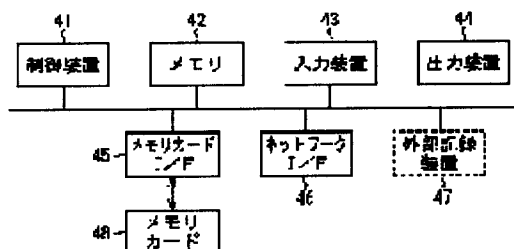
(72)Inventor : KASAI KAZUHIRO

(54) MEMORY CARD, DEVICE AND METHOD FOR FORMING IMAGE, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the reliability of image file data by preventing alteration in the image file data that is created by an image-forming device for storing into a memory card.

SOLUTION: When the image file data that is created by the image-forming device is to be stored into the memory card, a unidirectional function is used for calculating the message digest value of the image file data, a secret key is used for signing the message digest value, and the signature is stored into the memory card with the image file data, thus preventing the signature from being easily altered for improving the reliability of the image file data.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-10044

(P2002-10044A)

(43) 公開日 平成14年1月11日 (2002.1.11)

| (51) Int.Cl. | 識別記号 | F I | テーマコード* (参考) |
|---------------|-------|---------------|-------------------|
| H 0 4 N 1/21 | | H 0 4 N 1/21 | 5 B 0 3 5 |
| G 0 6 F 3/06 | 3 0 4 | G 0 6 F 3/06 | 3 0 4 H 5 B 0 6 5 |
| | | 3/08 | C 5 C 0 7 3 |
| G 0 6 K 19/10 | | G 0 6 K 19/00 | R 5 J 1 0 4 |
| 19/07 | | | N |

審査請求 未請求 請求項の数21 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願2000-184993(P2000-184993)

(22) 出願日 平成12年6月20日 (2000.6.20)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 笠井 一宏

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 孝悦

Fターム(参考) 5B035 AA13 BB09 BC00 CA38

5B065 BA09 PA13 PA20

5C073 AA03 AA06 AB04 AB05 CE04

CE10

5J104 AA09 LA03 LA05 LA06 NA02

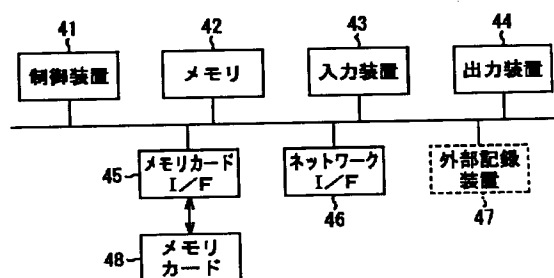
NA33 PA14

(54) 【発明の名称】 メモリカード、画像形成装置、画像形成方法及び記憶媒体

(57) 【要約】

【課題】 画像形成装置で作成してメモリカードに保存されている画像ファイルデータの改ざんを防止して、前記画像ファイルデータの信頼性を向上させる。

【解決手段】 画像形成装置で作成した画像ファイルデータをメモリカードに保存する際に、一方向性関数を用いて前記画像ファイルデータのメッセージダイジェスト値を算出し、秘密鍵を用いて前記メッセージダイジェスト値を署名し、前記署名を前記画像ファイルデータと一緒に前記メモリカードに保存することにより、署名の改ざんを行い難くして前記画像ファイルデータの信頼性を向上できるようにする。



(2)

特開2002-10044

1

2

【特許請求の範囲】

【請求項1】 画像形成装置により作成された画像ファイルデータの電子署名を記録可能な領域を有するメモリカードであって、

前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記電子署名が記録されるようになされていることを特徴とするメモリカード。

【請求項2】 画像形成装置により作成された画像ファイルデータに電子署名を施す際に使用する秘密鍵と、前記秘密鍵と対となる公開鍵とを記録可能な領域を有するメモリカードであって、
前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記秘密鍵及び公開鍵が記録されるようになされていることを特徴とするメモリカード。

【請求項3】 機器固有の秘密鍵を保持し、前記機器固有の秘密鍵を用いて電子署名を施すことを特徴とする画像形成装置。

【請求項4】 ユーザ定義による秘密鍵を新規に作成する秘密鍵作成手段を具備し、前記秘密鍵作成手段で作成した秘密鍵を用いて電子署名を施すことを特徴とする画像形成装置。

【請求項5】 メモリカードにアクセス可能なインターフェースを備えた画像形成装置において、
前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存手段を有することを特徴とする画像形成装置。

【請求項6】 前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴とする請求項5に記載の画像形成装置。

【請求項7】 前記機器固有の秘密鍵と対となる機器固有の公開鍵を保有することを特徴とする請求項5または6に記載の画像形成装置。

【請求項8】 前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成手段を有することを特徴とする請求項5～7の何れか1項に記載の画像形成装置。

【請求項9】 所定の画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に電子署名が記録されるようになされているメモリカードにアクセス可能なインターフェースを備えた画像形成装置において、
前記メモリカード内のプロパティファイルに、機器固有の公開鍵もしくは前記ユーザ定義による公開鍵の情報を保存する鍵情報保存手段を有することを特徴とする画像形成装置。

【請求項10】 前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する鍵情

報表示制御手段を有することを特徴とする請求項9に記載の画像形成装置。

【請求項11】 作成した画像ファイルデータをメモリカードに保存するデータ保存手段を有する画像形成装置であって、

前記画像ファイルデータに対して一方向性関数を用いて前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出手段と、

前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名手段と、

前記署名をメモリカード内のプロパティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存手段とを有することを特徴とする画像形成装置。

【請求項12】 ユーザ定義による秘密鍵を新規に作成する秘密鍵作成処理を行ない、前記秘密鍵作成処理で作成した秘密鍵を用いて電子署名を施すことを特徴とする画像形成方法。

【請求項13】 メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、

前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存処理を行うことを特徴とする画像形成方法。

【請求項14】 前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御処理を行うことを特徴とする請求項13に記載の画像形成方法。

【請求項15】 前記機器固有の秘密鍵と対となる機器固有の公開鍵を使用して電子署名を施すことを特徴とする請求項13または14に記載の画像形成方法。

【請求項16】 前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成処理を行うことを特徴とする請求項13～15の何れか1項に記載の画像形成方法。

【請求項17】 メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、

前記メモリカード内のプロパティファイルに、機器固有の公開鍵もしくはユーザ定義による公開鍵を保存する鍵情報保存処理を行うことを特徴とする画像形成方法。

【請求項18】 前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する表示制御処理を行うことを特徴とする請求項17に記載の画像形成方法。

【請求項19】 作成した画像ファイルデータをメモリカードに保存するデータ保存処理を行う画像形成方法であって、

前記画像ファイルデータに対して一方向性関数を用いて

(3)

特開2002-10044

3

4

前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出処理と、

前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名処理と、

前記署名をメモリカード内のプロパティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存処理とを行うことを特徴とする画像形成方法。

【請求項20】 前記請求項1～11の何れかに記載の各手段を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴とする記憶媒体。

【請求項21】 前記請求項12～19の何れか1項に記載の画像形成方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はメモリカード、画像形成装置、画像形成方法及び記憶媒体に関し、特に、画像ファイルデータの改ざんを防止するために用いて好適なものである。

【0002】

【従来の技術】従来、電子スチルカメラなどといった画像形成装置で作成した画像ファイルデータをメモリカードに保存する方法が行われている。前記メモリカードを用いて前記画像ファイルデータを印刷する場合であれば、プリンタと接続されたパーソナルコンピュータ（以下、PCと省略）もしくはプリンタ自体に、前記メモリカードにアクセス可能なインターフェース（以下、I/Fと省略）を備えれば、前記メモリカードを接続することによりプリントすることができる。

【0003】また、前記画像ファイルデータをパーソナルコンピュータ、あるいは電子手帳等に転送する場合であれば、メモリカードへアクセス可能なI/Fを備えた被転送装置に前記メモリカードを接続することにより、画像ファイルデータの授受を容易に行うことができる。

【0004】

【発明が解決しようとする課題】しかし、前記従来例の保存方法においては、以下のような問題があった。すなわち、メモリカード内に保存されている画像ファイルデータは電子的なデータであるため複製が容易である。そのため、不正複製、不正利用、改ざん等が行われる問題があった。したがって、前記メモリカードに保存されている画像ファイルデータが改ざんされたものではなく、正当なデータであることを証明する必要が出てきた。

【0005】そこで、本発明は画像形成装置にて画像ファイルデータをメモリカードに保存する際に、保存対象の画像ファイルデータに電子署名を施すことで、前記画

像ファイルデータの信頼性を向上させることを目的とする。

【0006】また、前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域に前記電子署名を記録することで、信頼性さらにを向上させることを目的とする。

【0007】また本発明は、メモリカード内に格納する画像ファイルデータの改ざんを防止し、そのデータの信頼性を向上させることを目的としている。

【0008】

【課題を解決するための手段】本発明のメモリカードは、画像形成装置により作成された画像ファイルデータの電子署名を記録可能な領域を有するメモリカードであって、前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記電子署名が記録されるようになされていることを特徴としている。また、本発明の他の特徴とするところは、画像形成装置により作成された画像ファイルデータに電子署名を施す際に使用する秘密鍵と、前記秘密鍵と対となる公開鍵とを記録可能な領域を有するメモリカードであって、前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記秘密鍵及び公開鍵が記録されるようになされていることを特徴としている。また、本発明のその他の特徴とするところは、機器固有の秘密鍵を保持し、前記機器固有の秘密鍵を用いて電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、ユーザ定義による秘密鍵を新規に作成する秘密鍵作成手段を具備し、前記秘密鍵作成手段で作成した秘密鍵を用いて電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、メモリカードにアクセス可能なインターフェースを備えた画像形成装置において、前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存手段を有することを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵と対となる機器固有の公開鍵を保有することを特徴としている。また、本発明のその他の特徴とするところは、前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成手段を有することを特徴としている。また、本発明のその他の特徴とするところは、所定の画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に電子署名が記録されるようになされているメモリカードにアクセス可能なインターフェースを備えた画像形成装置において、前記メモリカード内のプ

特開2002-10044

6

(4)

5

ロバティファイルに、機器固有の公開鍵もしくは前記ユーザ定義による公開鍵の情報を保存する鍵情報保存手段を有することを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴としている。また、本発明のその他の特徴とするところは、作成した画像ファイルデータをメモリカードに保存するデータ保存手段を有する画像形成装置であって、前記画像ファイルデータに対して一方向性関数を用いて前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出手段と、前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名手段と、前記署名をメモリカード内のプロパティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存手段とを有することを特徴としている。

【0009】本発明の画像形成方法は、ユーザ定義による秘密鍵を新規に作成する秘密鍵作成処理を行ない、前記秘密鍵作成処理で作成した秘密鍵を用いて電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵と対となる機器固有の公開鍵を使用して電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、前記メモリカード内のプロパティファイルに、前記機器固有の公開鍵もしくはユーザ定義による公開鍵を保存する鍵情報保存処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する表示制御処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、作成した画像ファイルデータをメモリカードに保存するデータ保存処理を行う画像形成方法であって、前記画像ファイルデータに対して一方向性関数を用いて前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出処理と、前記メッセ

ジダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名処理と、前記署名をメモリカード内のプロパティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存処理とを行うことを特徴としている。

【0010】本発明の記憶媒体は、前記に記載の各手段を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。また、本発明のその他の特徴とするところは、前記に記載の画像形成方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

【0011】

【発明の実施の形態】以下、本発明のメモリカード、画像形成装置、画像形成方法及び記憶媒体の実施の形態を図面を参照して説明する。

「第1の実施の形態」電子署名技術として現在、RSA (Rivest-Shamir-Adelman) 方式などのいわゆる非対称公開鍵方式を利用したものがある。前記非対称公開鍵方式は、「公開鍵」と「秘密鍵」という一対の鍵情報を設定している。

【0012】図13及び図14は、前記電子署名について概念的に説明したものである。この技術においては、図14中の「メッセージダイジェスト値」と「公開鍵」がポイントとなっている。前記メッセージダイジェスト値は、個々のメッセージに対し固有の値を有している。

【0013】まず、署名したいデータ（テキストやバイナリ）に対して、メッセージダイジェスト値を算出する。前記メッセージダイジェスト値は、一方向性関数（ハッシュ関数）を用いて、署名したいデータから作成されるものであり、署名したいデータに固有の値である。そして、前記のように作成されたメッセージダイジェスト値を秘密鍵で暗号化する。

【0014】電子的データの送受信を行う場合、送信側は前記秘密鍵で暗号化されたメッセージダイジェスト値を署名として、署名対象データと一緒に受信側に送り出す。受信側は、受信した署名データを署名側の公開鍵で復号化してメッセージダイジェスト値を得る。そして、受信した署名対象データから算出されるメッセージダイジェスト値と、前記復号化したメッセージダイジェスト値とを比較する。前記のような手順で署名の検証を行うことができる。以下、本実施の形態の更に詳細に説明する。図1は、本実施の形態にかかわる画像ファイルデータの改ざん防止機能を備えた画像形成装置の構成を示すブロック図である。この画像装置は、制御装置（CPU）41、メモリ42、入力装置43、出力装置44、メモリカードI/F45、とからなる。そして、この画像形成装置は状況に応じてネットワークI/F46、外部記録装置47をも含むことがある。

【0015】制御装置41は、この画像形成装置の各部

(5)

特開2002-10044

7

の動作を統括して管理するものであり、マイクロプロセッサ及びその周辺回路で構成されている。メモリ42は、例えばROM (Read Only Memory)、RAM (Random Access Memory) 等があり、この画像形成装置で実行されるプログラム、処理に用いられるデータ、ユーザが作成したデータ等が格納されている。

【0016】入力装置43は、例えばキーボード、ポインティングデバイス、タッチパネル等に相当し、制御装置41に対して各種の動作を指示するために用いられる。出力装置44は、例えばCRT、液晶表示装置等に相当し、システムからのメッセージや視覚化されたモデル図などが表示される。

【0017】メモリカードI/F45は、メモリカード48に蓄積されているデータを読みとったり、メモリ42に蓄積されているデータをメモリカード48に書き込んだりするものである。

【0018】外部記録装置47は、例えば磁気ディスク装置、光ディスク装置、光磁気ディスク装置等であり、上述のプログラムやデータを保存しておき、必要に応じてそれらをメモリ42にロードして使用することができる。

【0019】ネットワークI/F46は、LAN、モデム等の任意のネットワーク(回線)を介して外部の装置と通信をする。これにより、必要に応じて前記プログラムや前記データを外部の装置からネットワークを介して受け取り、それらをメモリ42にロードして使用することができる。

【0020】一方、図2はメモリカード48のメモリマップの一例を示す図であり、画像ファイルデータ、画像ファイルデータの署名及びプロパティファイルが保存されている。プロパティファイルは、基本的にASCIIコードのみで使用したText形式により記載されており、画像ファイルを印刷したい場合はプリントジョブごとに指定情報が完結する記述となっている。

【0021】また、プロパティファイルは、メモリカード48内に1つ存在し、対象となる画像ファイルデータは保存場所を問わない。さらに、本実施の形態においては、どの画像形成装置でも書きこみ可能な通常領域と、アクセス権利の設定を行うことにより、指定された、若しくはアクセス権利の設定を行なった画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域を設定し、ユーザの判断で画像ファイルデータや画像ファイルデータの署名などを保存することができるようにしている。

【0022】次に、前記構成からなる第1の実施の形態に関わる画像ファイルデータの改ざん防止を行うために、画像形成装置に配設されている制御手段の一例について、図1の装置構成ブロック図及び図3のフローチャートを用いて説明する。

【0023】本実施の形態では、図4に示すように、M

8

D5と呼ばれるハッシュ関数を用いて署名したいデータのメッセージダイジェスト値を算出するようにしている。MD5は現在、暗号化プログラムの1つであるPGP (Pretty Good Privacy) で実際に使われているメッセージダイジェスト関数である。

【0024】画像形成装置にて、ユーザが作成した画像ファイルデータをメモリカード48に保存しようとするとき、ユーザは入力装置43よりその保存処理を指示し、その信号が制御装置41に入力されることにより制御が開始される。

【0025】制御装置41は、そのデータに電子署名を行うかどうかユーザに確認するため、出力装置44にその意向を表示する(ステップS61)。図5は、この意向表示の一例を示す図であり、これに限定されるものではない。署名を行わない場合は、すぐさまメモリカード48の通常領域にその画像ファイルデータを保存して制御処理を終了する(ステップS66)。

【0026】一方、署名を行う場合、署名対象画像ファイルデータのメッセージダイジェスト値を算出し(ステップS62)、前記メッセージダイジェスト値を前記画像形成装置が保有している機器固有の秘密鍵で暗号化し(ステップS63)、この暗号化されたメッセージダイジェスト値を署名としてメモリカード48の対象装置以外書き込み不可領域に保存する(ステップS64)。尚、この機器固有の秘密鍵と対となる機器固有の公開鍵も画像形成装置に保有されている。

【0027】最後に、署名対象となった画像ファイルデータをメモリカード48の対象装置以外書き込み不可領域に保存し(ステップS65)、制御処理を終了する。これらの署名や、署名対象となった画像ファイルデータの保存領域をユーザに選択させるようにしても良い。

【0028】また、本実施の形態によれば、画像ファイルデータをメモリカードに保存する際に、一方向性関数を用いて前記画像ファイルデータのメッセージダイジェスト値を算出し、秘密鍵を用いて前記メッセージダイジェスト値を署名し、前記画像ファイルデータと一緒に前記メモリカードに保存するようにしたので、前記画像ファイルデータの改ざんを確実に防止することができ、前記画像ファイルデータの信頼性を向上させることができる。

【0029】「第2の実施の形態」前述した第1の実施の形態では、機器固有の秘密鍵、機器固有の公開鍵を用いて行う電子署名方式について述べたが、この第2の実施の形態では、ユーザが定義した秘密鍵、公開鍵を用いての電子署名を行う方式について説明する。

【0030】この第2の実施の形態に関わる画像ファイルデータの改ざん防止方法を備えた画像形成装置の制御手順の一例について、図1の装置構成ブロック図、及び図6のフローチャートを用いて説明する。

【0031】ユーザが作成した画像ファイルデータをメ

50

メモリカード48に保存しようとするとき、ユーザは入力装置43よりその保存処理を指示し、その信号制御装置41に入力されることにより制御が開始される。

【0032】制御装置41は、そのデータに電子署名を行うかどうかをユーザに確認するため、出力装置44側にその意向を表示する(ステップS71)。署名を行わない場合は、すぐさまメモリカード48の通常領域にその画像ファイルデータを保存して制御処理を終了する。

【0033】一方、署名を行う場合、制御装置41はユーザに対して、機器固有の秘密鍵を用いるか、新たにユーザ定義による秘密鍵を作成するか、出力装置44にその意向を表示する(ステップS72)。

【0034】図7は、この意向表示の一例を示す図であるが、これに限定されるものではない。ユーザ定義による秘密鍵を作成する場合、制御装置41はユーザに対して任意の暗証番号を入力してもらい(ステップS73)、入力された暗証番号を基にユーザ定義による秘密鍵を自動的に作成する(ステップS74)。

【0035】この後、前記ユーザ定義による秘密鍵よりユーザ公開鍵が自動的に生成される(ステップS75)。以降、署名対象画像ファイルデータのメッセージダイジェスト値を算出し(ステップS76)、前記メッセージダイジェスト値を選択された機器固有の秘密鍵もしくはユーザ定義による秘密鍵で暗号化し(ステップS77)、暗号化されたメッセージダイジェスト値を署名としてメモリカード48の対象装置以外書き込み不可領域に保存する(ステップS78)。

【0036】最後に、署名対象となった画像ファイルデータをメモリカード48の対象装置以外書き込み不可領域に保存し(ステップS79)、制御処理を終了する。これにより、機器固有となる秘密鍵、公開鍵以外の秘密鍵、公開鍵を使用することができる。

【0037】また、本実施の形態によれば、ユーザ定義による秘密鍵を新規に作成して電子署名を施すようにしたので、改ざんされ難い電子署名を行うことができる。

【0038】また、本実施の形態によれば、署名するために用いる秘密鍵をユーザが作成できることにより、機器固有の秘密鍵、公開鍵以外の秘密鍵、公開鍵を使用することができるので、署名された画像ファイルデータの信頼性をより向上させることができる。前述した第2の実施の形態では、ユーザ定義による秘密鍵を新たに作成することにより、機器固有の秘密鍵以外の秘密鍵を用いて電子署名を施す方法について説明した。この第3の実施の形態では、ユーザ定義による秘密鍵、ユーザ公開鍵が画像形成装置に保存されており、それらを利用する方法について説明する。

【0039】「第3の実施の形態」この第3の実施の形態に関わる画像ファイルデータの改ざん防止方法を備えた画像形成装置の制御手順の一例について、図1の装置構成ブロック図、及び図8のフローチャートを用いて説

明する。

【0040】ユーザが作成した画像ファイルデータをメモリカード48に保存しようとするとき、ユーザは入力装置43よりその保存処理を指示し、その信号制御装置41に入力されることにより制御が開始される。

【0041】制御装置41は、そのデータに電子署名を行うかどうかユーザに確認するため、出力装置44にその意向を表示する(ステップS801)。署名を行わない場合は、すぐさまメモリカード48の通常領域にその画像ファイルデータを保存して制御処理を終了する。

【0042】一方、署名を行う場合、制御装置41はユーザに対して、機器固有の秘密鍵を使用するか、機器に保存されているユーザ定義による秘密鍵を使用するか、新たにユーザ定義による秘密鍵を作成するか、出力装置44にその意向を表示する(ステップS802)。図9は、この意向表示の一例を示す図であるが、これに限定されるものではない。ユーザ定義による秘密鍵を使用しない場合は、前記第1の実施例に準ずる。

【0043】新たにユーザ定義による秘密鍵を作成する場合は、前記第2の実施の形態に従って秘密鍵暗証番号の入力を行ない(ステップS803)、秘密鍵、公開鍵を作成した後、前記秘密鍵、前記公開鍵を外部記録装置46もしくはメモリ42に保存する(ステップS804)。ただし、前記保存された秘密鍵、公開鍵は、ユーザの判断により、外部記録装置46またはメモリ42から削除することも可能である。

【0044】一方、ステップS802の判定の結果、秘密鍵を新規に作成しない場合にはステップS813に進み、登録済みの秘密鍵を使用するか否かを判断する。この判定の結果、機器に保存されているユーザ定義による秘密鍵を使用する場合、その秘密鍵に設定されている暗証番号を入力し(ステップS806)、この秘密鍵が前記ユーザのものであるか否かを検証する(ステップS807)。ここで、保存されているユーザ定義による秘密鍵が複数ある場合は、どれか1つをユーザに選択させ、その選択された秘密鍵の検証を行う。そして、前記ユーザのものと認証された場合は、前記秘密鍵と対となる公開鍵が外部記憶装置46またはメモリ42に存在するか確認し(ステップS808)、存在しなければ自動的に公開鍵を作成し、外部記憶装置46またはメモリ42に保存する(ステップS805)。

【0045】そして、ステップS809では、署名対象画像ファイルデータのメッセージダイジェスト値を算出し、前記メッセージダイジェスト値を前記ユーザ定義による秘密鍵で暗号化し(ステップS810)、暗号化されたメッセージダイジェスト値を署名としてメモリカード48に保存する(ステップS811)。最後に、署名対象となった画像ファイルデータをメモリカード48に保存し(ステップS812)、制御処理を終了する。

【0046】「第4の実施の形態」これまでの実施の形

(7)

特開2002-10044

11

態では、メモリカード48に署名対象画像ファイルデータと署名のみを保存していた。この第4の実施の形態では、署名を確認するための公開鍵と秘密鍵を、メモリカード48に保存する方法、画像形成装置の出力装置44に表示する方法について説明する。

【0047】この第4の実施の形態に関わる画像ファイルデータの改ざん防止方法を備えた画像形成装置の制御手順の一例について、図1の装置構成ブロック図、及び図10のフローチャートを用いて説明する。

【0048】ユーザが作成した署名対象画像ファイルデータ及び署名をメモリカード48に保存する手順はこれまでの実施の形態と同様である。この後、制御装置41は前記画像ファイルに使用した秘密鍵及びその対となる公開鍵をメモリカード48に保存するか、表示装置に表示するかをユーザに確認するため、出力装置44にその意向を表示する(ステップS901)。図11は、この意向表示の一例であるが、これに限定されるものではない。

【0049】次に、秘密鍵、公開鍵の保存、表示方法について選択する項目が出力装置側に現れる(ステップS902)、図12は、この意向表示の一例であるが、これに限定されるものではない。特に、公開鍵は前記画像ファイルデータと前記署名との検証に用いられるため、何らかの方法で保存しておく必要がある。これらの扱いについては、以下のような選択肢がある。

【0050】(公開鍵について)

(1) 公開鍵を画像ファイルデータと署名が保存されているメモリカード48と同一のメモリカード48に保存する。

(2) 公開鍵を画像ファイルデータと署名が保存されているメモリカード48と別のメモリカードに保存する。

(3) 公開鍵を出力装置に表示する。

【0051】(秘密鍵について)

(1) 秘密鍵を画像ファイルデータと署名が保存されているメモリカード48と同一のメモリカードに保存する。

(2) 秘密鍵を画像ファイルデータと署名が保存されているメモリカード48とは別のメモリカードに保存する。

(3) 秘密鍵を出力装置に表示する。

【0052】ステップS903及びステップS909の質問に応じて、前記秘密鍵、前記公開鍵の保存・表示方法を選択した後、前記秘密鍵、前記公開鍵を署名付き画像ファイルデータを保存しているメモリカード48と同一メモリカードに保存する(ステップS904及びS910)。

【0053】また、ステップS915の質問に応じて前記秘密鍵及び公開鍵を、署名付き画像ファイルデータと別のメモリカードに保存する場合、メモリカード48を交換するようユーザに指示した後に、交換されたメモリ

12

カード48を認識後、前記秘密鍵及び公開鍵を保存する(ステップS916及びS917)。

【0054】また、ステップS905の質問に応じて、秘密鍵をデータとは別メモリカードに保存する場合には、ステップS906において秘密鍵保存フラグをONにする。また、ステップS911の質問に応じて、公開鍵をデータとは別メモリカードに保存する場合には、ステップS912において公開鍵保存フラグをONにする。

【0055】ステップS907及びステップS913の質問に応じて前記秘密鍵及び公開鍵を出力装置44に表示する場合、前記秘密鍵、前記公開鍵を出力装置に表示する(ステップS908及びステップS914)。前記秘密鍵、前記公開鍵を保存、及び表示した後、制御装置41は処理を終了する。これらの秘密鍵や公開鍵は、ユーザの選択によりメモリカード48の前記画像形成装置以外書き込み不可領域に保存することもできる。

【0056】また、本実施の形態によれば、ユーザが作成した秘密鍵、公開鍵を画像形成装置に保存することにより、前記秘密鍵、前記公開鍵を再利用する際に、より容易に利用できることができる。

【0057】また、本実施の形態によれば、署名に用いた秘密鍵やその対となる公開鍵をメモリカードに保存したり前記秘密鍵、前記公開鍵を画像形成装置の出力装置に表示することにより、ユーザは前記秘密鍵、前記公開鍵を保管することができ、検証時に前記公開鍵を容易に用いることができたり、前記秘密鍵を再利用することができる。

【0058】(本発明の他の実施の形態)本発明は複数の機器(例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等)から構成されるシステムに適用しても1つの機器からなる装置に適用しても良い。

【0059】また、上述した実施の形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ(CPUあるいはMPU)に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【0060】また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピー(登録商標)ディスク、ハードディスク、光ディスク、光磁気ディスク、C

(8)

特開2002-10044

13

D-RROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0061】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態で説明機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【0062】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部または全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれる。

【0063】また、上記各実施の形態によれば、ユーザの選択によりメモ리카ードの前記画像形成装置以外書き込み不可領域に署名、画像ファイルデータ、秘密鍵、公開鍵を保存することもでき、それらのファイルのセキュリティを向上させることができる。

【0064】

【発明の効果】以上説明したように、本発明によれば、画像形成装置で作成してメモ리카ードに保存されている画像ファイルデータの改ざんを有効に防止することができ、前記画像ファイルデータの信頼性を大幅に向上させることができる。

【図面の簡単な説明】

【図1】画像ファイルデータの改ざん防止機能を備えた画像形成装置の構成例を示すブロック図である。

【図2】メモ리카ードのメモリマップの一例を示す説明*

*図である。

【図3】第1の実施の形態の画像形成装置の処理手順を説明するフローチャートである。

【図4】電子的データとメッセージダイジェスト値との関連を説明する図である。

【図5】第1の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図6】第2の実施の形態の画像形成装置の処理手順を説明するフローチャートである。

【図7】第2の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図8】第3の実施の形態の画像形成装置の処理手順を説明するフローチャートである。

【図9】第3の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図10】第4の実施の形態を説明するフローチャートである。

【図11】第4の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図12】第4の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

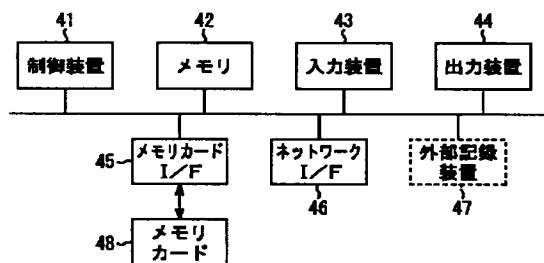
【図13】電子署名に関する説明図である。

【図14】電子署名に関する説明図である。

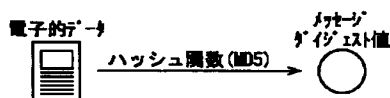
【符号の説明】

- 41 制御装置
- 42 メモリ
- 43 入力装置
- 44 出力装置
- 45 メモ리카ード I/F
- 46 ネットワーク I/F
- 47 外部記憶装置
- 48 メモ리카ード

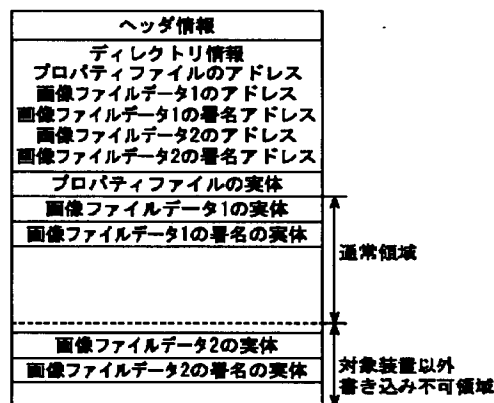
【図1】



【図4】



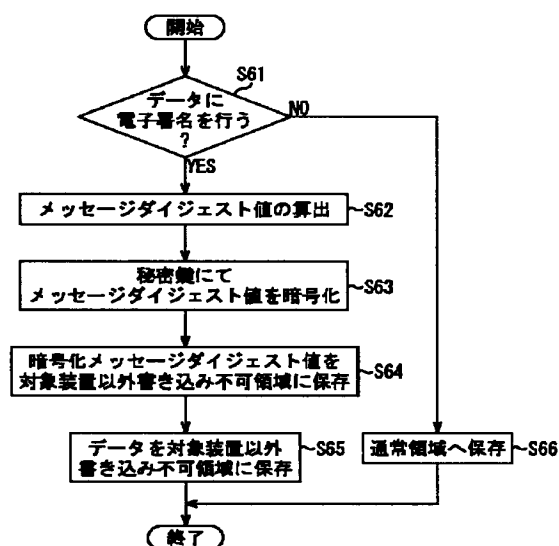
【図2】



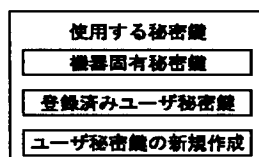
(9)

特開2002-10044

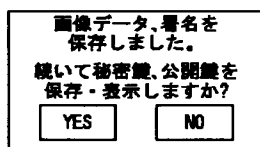
【図3】



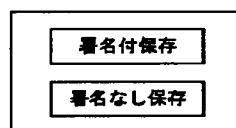
【図9】



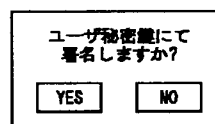
【図11】



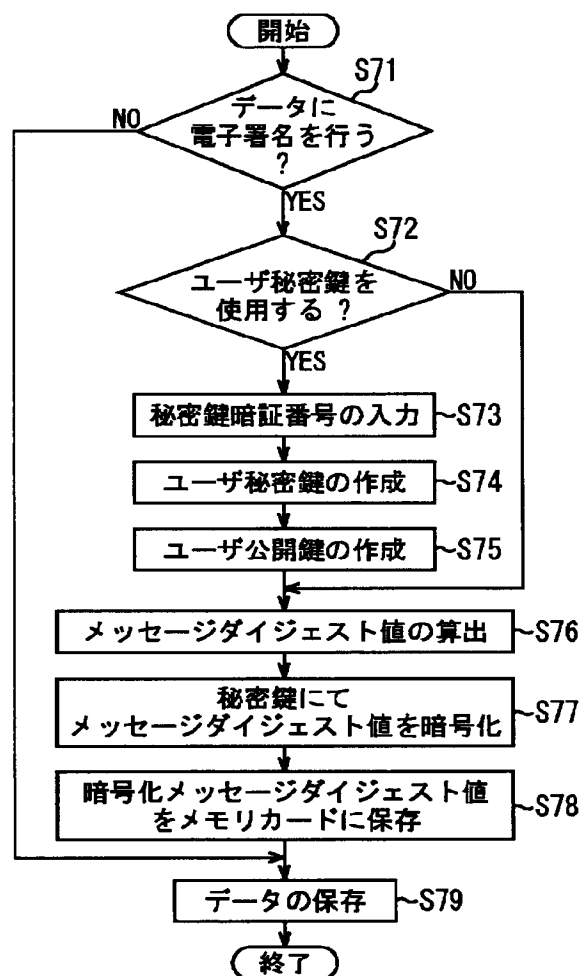
【図5】



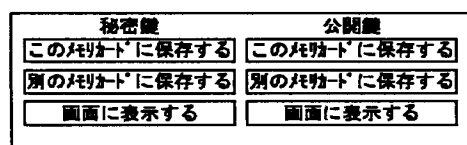
【図7】



【図6】



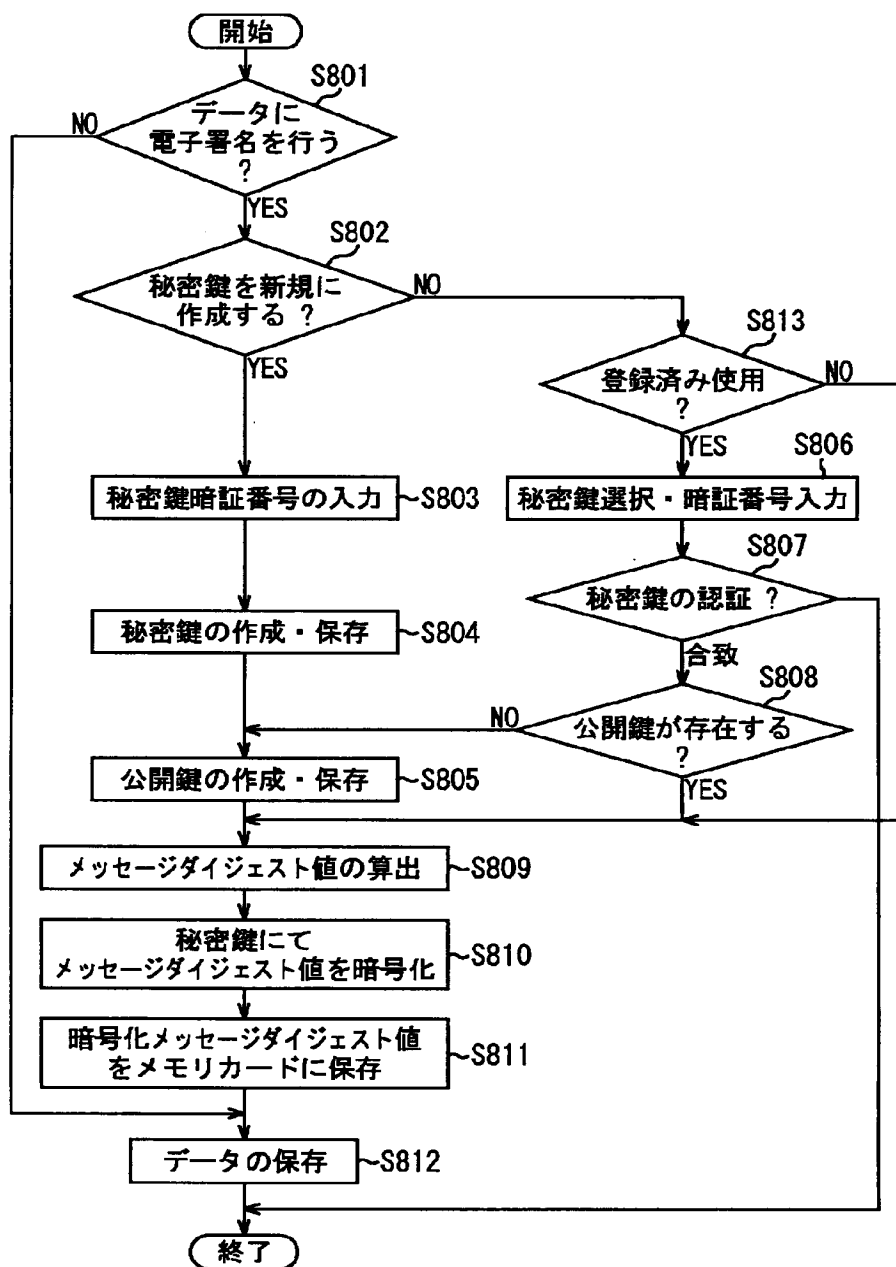
【図12】



(10)

特開2002-10044

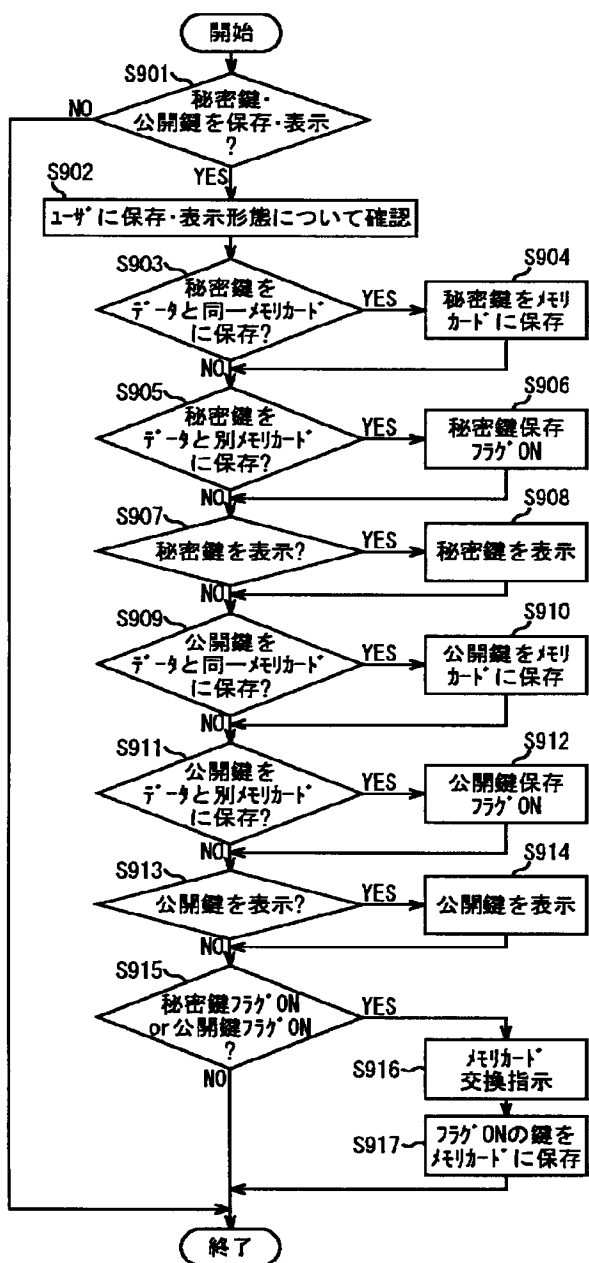
【図8】



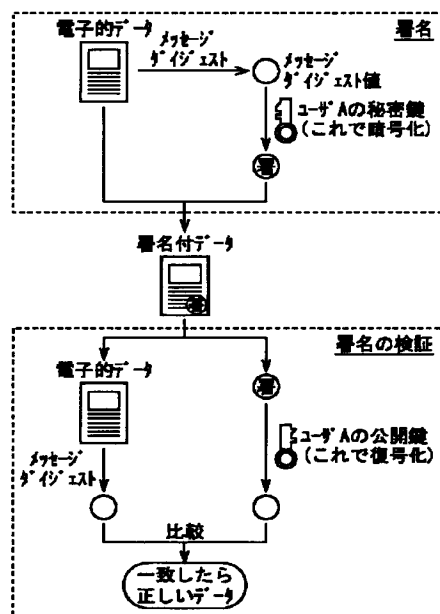
(11)

特開2002-10044

【図10】



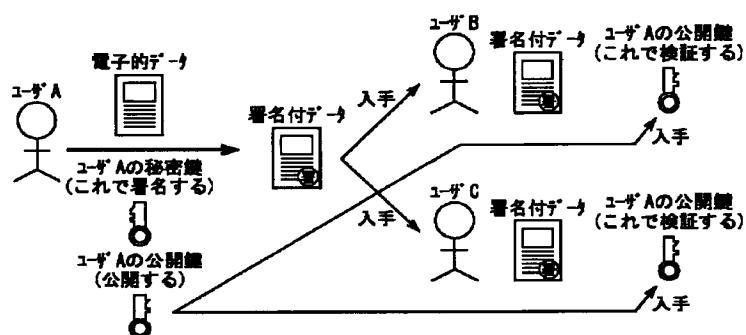
【図14】



(12)

特開2002-10044

【図13】



フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テーマコード (参考)

// H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 B